REMARKS

The non-final Office Action, mailed November 17, 2006, considered claims 1-25. Claims 4 and 6 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,510,236 to Crane et al., hereinafter *Crane*. Claims 1-3, 11-13, 15-19 and 21-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2002/0112155 to Martherus et al., hereinafter *Martherus*. Claims 7-8 were rejected under 35 U.S.C. § 103(a) over *Crane*. Claims 5 and 9-10 were rejected under 35 U.S.C. § 103(a) over *Crane* and *Martherus*. Claims 14 and 20 were rejected over *Martherus*, *Crane*, and further in view of U.S. Patent No. 6,324,571 to Hacherl.[1]

By this amendment claims 1, 3-11, 17 and 21-25 have been amended, of which claims 1, 4, 11, 17 and 21 are the only independent claims at issue.[2]

The present invention is generally directed to controlling authentication of principals for access to network resources in a network environment. For example, claim 11 defines receiving at the super authority a request for an authenticating authority resolution from one of a plurality of authenticating authorities, wherein the request comprises an account ID of a principal to be authenticated. Next, claim 11 defines accessing an assignment mapping that maps each account ID in a plurality of account IDs to a corresponding plurality of authenticating authorities that can be used to authenticate the account ID, the account ID comprising the identity of the principal. Next, claim 11 defines locating within the mapping an identity of an assigned authenticating authority from among the one or more authenticating authorities that corresponds to the account ID of the principal to be authenticated. Lastly, claim 11 defines causing an authentication request to be transmitted to the assigned authenticating authority located from among the one or more authenticating authorities, the assigned authenticating authority having been located using the principal's account ID, wherein the request asks the assigned authenticating authority to authenticate the principal.

Claim 1 is a method claim similar to claim 11, but from the perspective of an authenticating authority. Claim 4 is a system claim similar to claim 11. Claim 17 is an apparatus

---

[1] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[2] Support for the amendments to the claims are found throughout the specification and previously presented claims, including but not limited to paragraphs [0028], [0031], [0036], [0040], [0041], [0046] and Figures 3B, 4B & 5.

claim that corresponds to claim 11. Claim 21 is a computer program product claim corresponding to claim 11. Applicants respectfully submit that the cited art of record does not anticipate or otherwise render the amended claims unpatentable for at least the reason that the cited art does not disclose, suggest, or enable each and every element of these claims.

Crane describes an authentication framework for authenticating clients (Abs.). Within the framework, a method is performed that involves a client sending an authentication request to an application server where the request includes a user ID and a device ID. The application server determines which device authentication server the request is for based solely on device type and forwards the request (including the device ID and the user ID) to that server (Col. 2:28-38, Col. 4:64-Col. 5:26). The application server manages authentication requests from multiple clients having various authentication devices (e.g. biometric devices such as fingerprint or iris scanners) (Col 2:1-4). Essentially, the application access server acts as a "traffic cop" or router for the various requests from the different authenticating devices based on the device paradigm, or the data originating from the authenticating device (Col. 3:14-24, 37-46).

Martherus describes authenticating a user for multiple resources distributed across multiple domains using a single authentication (Abs.). The described method receives a request for a protected resource in a first domain. The system then redirects the request to a second domain for authentication. The user is authenticated for the first domain at the second domain (par. [0012]). The second domain transmits an authentication cookie to the user that allows the user to authenticate to a third domain. Then, when the user requests authentication to the third domain, the system uses the cookie from the second domain to authenticate to the third domain (par. [0011]-[0012]).

Neither *Crane* nor *Martherus* teaches or suggests accessing an assignment mapping that maps each account ID in a plurality of account IDs to a corresponding plurality of authenticating authorities that can be used to authenticate the account ID, the account ID comprising the identity of the principal, as recited in claim 11. Furthermore, Neither *Crane* nor *Martherus* teaches or suggests causing an authentication request to be transmitted to the assigned authenticating authority located from among the one or more authenticating authorities, the assigned authenticating authority having been located using the principal's account ID, wherein the request asks the assigned authenticating authority to authenticate the principal, as recited in claim 11. At least for either of these reasons, claim 11 patentably defines over the art of record.

At least for either of these reasons, claims 1, 4, 17 and 21 also patentably define over the art of record. Since each of the dependent claims depend from one of claims 1, 4, 11, 17 and 21, each of the dependent claims also patentably define over the art of record for at least either of the same reasons.

Claims 4-10 were rejected under 35 U.S.C. § 101 because it is alleged that a "controlling authority" would reasonably be interpreted by one of ordinary skill in the art as software, per se, and is thus functional descriptive material. Claims 4-10 have been amended to include a system with memory, a processor and computer-readable media having stored thereon computer-executable instructions. Accordingly, Applicants respectfully request that the 35 U.S.C. § 101 rejection to claims 4-10 be withdrawn.

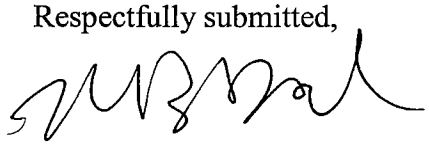
Claims 21-25 were rejected under 35 U.S.C. § 101 because they recite non-statutory subject matter. Claims 21-25 have been amended to recite "recordable-type computer-readable media." Accordingly, Applicants respectfully request that the 35 U.S.C. § 101 rejection of claims 21-25 be withdrawn.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

Dated this 16th day of February, 2007.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
MICHAEL B. DODD
Registration No. 46,437
Attorneys for Applicant
Customer No. 47973

GRL:ds
DS0000007106V001